ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 19 Introduction to Communication Systems
Graded Homework 3. **Due Date: December 4, 2008** November 27, 2008

PROBLEM 1. 1. Let a, b, m be positive integers and let $d = \gcd(a, m)$.

(a) Assume that d divides b. Prove that the congruence equation

$$ax \equiv b \pmod{m}$$

has an integer solution for x.

(b) Assume that the congruence equation

$$ax \equiv b \pmod{m}$$

has an integer solution for x, then prove that d must divide b.

2. Let a, b, c, m be positive integers. Assume that

$$ac \equiv bc \pmod{m}.$$

Prove that

$$a \equiv b \left(\mod \frac{m}{\gcd(c, m)}\right).$$

PROBLEM 2. Bruce Lee goes to a pet store and buys 5 rabbits. On his way home he decides to buy some food for the rabbits. He has k francs in his wallet. Each piece of rabbit food costs one franc. Upon reaching the food store he realizes that he needs twice the amount of money he has in his wallet to buy sufficient food for 5 rabbits. He goes to the ATM and withdraws k more francs. Upon reaching his house he divides the pieces of rabbit food equally amongst all the rabbits to find out that 4 number of pieces were left over. Note that we cannot divide a piece of rabbit food into smaller pieces.

One week later Bruce finds out that there are 35 rabbits in total. He goes to the food store to buy some more food. He again has k francs in his wallet and realizes that he needs five times that amount to buy sufficient pieces of food for all the rabbits. Again, upon equally dividing the food amongst all the rabbits he finds out that 30 pieces are left over.

What was the original amount of money k, Bruce Lee had in his wallet ? (Hint: Use part 2 of Problem 1.)

PROBLEM 3. Let m be some positive integer. Let $a, b \in \mathbb{N}_m$, i.e., we can think of $a, b \in \{0, 1, \ldots, m-1\}$. Assume that we can compute the multiplication $|a \cdot b|_m$ in one operation. Show that you can compute $|a^{30890123}|_m$ in at most $2 \log_2 30890123$ operations.

Problem 4 (RSA with symbols combined). NOTE: For this problem feel free to use a calculator, MATLAB or any other computing software.

We have a text in English and we will encrypt it using the RSA algorithm as follows.

We first break the plaintext into groups of 3 letters each. We then use a map which converts each group of three letters into a number. We define the map as follows. As usual, we associate each of the 26 letters of the alphabet with a number:

$$A = 0, B = 1, \ldots Z = 25$$

Enumerate all the possible groups of 3 letters in a lexicographical order. More precisely, we start with AAA and end with ZZZ. Clearly, there are $26^3 = 17576$ such groups. To AAA we associate the number 0, to AAB we associate 1, to ABA we associate 26, and so forth. Finally, to ZZZ we associate 17575.

We now apply an RSA encryption to these numbers. Let $m = 131 \times 137$ and let the public key be $K = 49$.

1. What is the secret key k ?
2. Suppose one group of the plaintext is given by $\alpha\beta\gamma$ where $\alpha, \beta, \gamma \in \{A, B, C, \ldots, Z\}$. Then what is the number corresponding to this plaintext before encryption? E.g., what is the number corresponding to "THE". (Hint: It better be between 0 and 17575.)
3. Decrypt the following ciphertext, $2086, 14863$.

Problem 5 (Digital Signatures Using RSA). Yakari is in love with Asquare and wants to send her a poem. Unfortunately Yakari's malicious friend Babubhai likes to pass himself off as Yakari and sends fake messages to Asquare. So in order to save his love story, Yakari decides to "digitally sign" his poem using an RSA scheme. Let m be the modulus, let K be the public key and let k be the private key. Let the poem be the plaintext P. At the end of his poem P Yakari appends the "signature" $C = E_k(P)$, i.e., he appends the ciphertext corresponding to P, but using his *private* key for the encryption.

When Asquare receives the signed message, she uses Yakari's public key (K, m) and decrypts the signature C to compute $D_K(C)$. She then compares $D_K(C)$ with the message P in order to verify that the message was sent by her true love Yakari.

Show that $D_K(C)$ is indeed equal to P and argue why this scheme will save their love story.